LIVRE BLANC

Résilience opérationnelle dans le Cloud

Pourquoi les dirigeants et les régulateurs des services financiers sont-ils inquiets, et ce que vous pouvez faire à ce sujet.

Graham Corr, Senior Industry Consultant,
EMEA Financial Services Practice

teradata.

Table des matières

Les données au cœur de la résilience opérationnelle

Il est 7 h du matin et la journée de travail commence à peine lorsque votre fournisseur de Cloud met à jour sa page d'état pour annoncer une panne de courant dans un centre de données. Vos services seront-ils affectés ? Lesquels ? Pendant combien de temps ? Pouvez-vous maintenir vos opérations critiques ? Quelles seront les conséquences si vous ne le pouvez pas ?

On ne peut pas prédire comment et où se produira la prochaine panne, ni se préparer à toute éventualité. La résilience opérationnelle dans un monde connecté axé sur le Cloud est le défi qui empêche les dirigeants et les régulateurs des services financiers de dormir la nuit. Trop dépendre d'une poignée de prestataires mondiaux génère de nouveaux risques systémiques pour le secteur. Il est temps d'agir.

Déplacer des applications et des opérations vers le Cloud ne signifie pas que la résilience opérationnelle est « intégrée ». Le recours à des implémentations sur un « Cloud unique » ou en « Cloud uniquement » augmente le risque de perturbation si un fournisseur subit une panne. Et, comme on l'a vu récemment, même les plus grands fournisseurs de Cloud peuvent rencontrer plusieurs pannes pour diverses raisons. Des experts indépendants ont enregistré 21 pannes distinctes sur les principales plateformes Cloud en 2020, et en 2021 la situation fut sensiblement la même, AWS, Microsoft, Google et Facebook ayant tous connu de graves pannes.

Les organismes financiers doivent investir dans leur propre résilience opérationnelle pour absorber les chocs et réagir rapidement afin de maintenir leurs opérations en toutes circonstances.

La résilience opérationnelle exige une connaissance détaillée des risques liés au flux de données dans l'entreprise et des plans précis d'accès, de récupération et d'utilisation continue des données pour assurer continuité des fonctions critiques.

Les régulateurs recherchent de plus en plus des preuves de résilience, et les coûts liés à l'impossibilité de fournir des services commerciaux importants pourraient être catastrophiques. Dans tout plan de résilience opérationnelle, il est crucial de maintenir l'accès aux données critiques.

teradata.

Comprendre la résilience opérationnelle dans le nouveau paysage du Cloud

Le Cloud offre nombre d'occasions et d'avantages aux organismes financiers. En conséquence, de plus en plus d'entreprises transfèrent davantage de charges de travail vers le Cloud.

- Entre 40 et 90 % des charges de travail des banques mondiales pourraient être hébergées dans un Cloud public ou un logiciel as-a-service d'ici 10 ans.[1]

L'efficacité et les économies du Cloud ne laissent aucun doute. Cependant, les opérations centrées sur le Cloud introduisent de nouveaux risques et soulèvent des défis différents pour les acteurs chargés de maintenir la résilience opérationnelle. La gestion des données et des charges de travail dans le Cloud nécessite un certain contrôle en échange d'économies et d'une certaine flexibilité. Il est important de comprendre le sens de ces compromis pour la résilience opérationnelle ; les stratégies axées sur le Cloud ne doivent pas devenir des stratégies « Cloud uniquement » sans une analyse détaillée de ces nouveaux risques.

Risques commerciaux du Cloud

Passer au Cloud signifie travailler avec de nouveaux partenaires et leur confier vos données. Bien comprendre les conditions générales qui régissent ces relations est essentiel pour maintenir la résilience opérationnelle. Est-il facile de rapatrier des données des partenaires Cloud si nécessaire ? Combien cela coûtera-t-il ?

Les organisations financières doivent également évaluer l'impact sur la résilience opérationnelle des conditions générales imposées par les fournisseurs de services Cloud (CSP).

- À l'échelle mondiale, près des deux tiers de tous les services Cloud (61 %) sont fournis par trois grandes entreprises technologiques (Amazon, Microsoft et Google).[2]
- 70 % des banques et 80 % des assureurs s'appuient sur seulement deux fournisseurs de Cloud pour l'IaaS (Infrastructure as a service).[3]

Cette concentration donne aux grandes entreprises technologiques un pouvoir important pour fixer leurs conditions et définir la nature de leurs relations commerciales. Leurs modalités sont-elles compatibles avec la gouvernance interne et la conformité, et conformes aux plans de résilience opérationnelle ? L'entreprise a-t-elle la flexibilité requise pour être résiliente ou est-elle liée à un seul fournisseur qui peut dicter ses conditions commerciales ?

> **« Ce pouvoir concentré sur les conditions peut se manifester avec secret et opacité, et ne pas fournir aux clients le type d'informations dont ils ont besoin pour surveiller les risques dans leur service. »**
>
> Andrew Bailey, Gouverneur de la Banque d'Angleterre[4]

Les aspects commerciaux de la résilience opérationnelle doivent aussi tenir compte de la protection des données et de l'exposition aux cyber-risques. Bien que les fournisseurs de services Cloud aient réalisé d'importants investissements dans la confidentialité des données et la cybersécurité, personne n'est à l'abri des attaques.

En outre, la conformité au RGPD et aux statuts similaires de protection des données personnelles doit rester au cœur de la résilience opérationnelle. Savoir exactement où résident les données et être en mesure de prouver que tout transfert de données est entièrement conforme à la législation locale est essentiel. Cela inclut les déplacements vers et entre les fournisseurs de services Cloud.

1 https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report

2 https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

3 https://www.imf.org/en/News/Articles/2021/06/16/sp061721-bigtech-in-financial-services

4 https://www.reuters.com/business/retail-consumer/bank-england-crack-down-secretive-cloud-computing-services-2021-07-13

teradata.

Par exemple, l'arrêt Schrems II de la Cour de justice de l'Union européenne (CJUE) impose clairement aux entreprises la responsabilité d'assurer des niveaux supplémentaires de protection des données personnelles si les fournisseurs de services Cloud ne peuvent pas garantir cette protection.[5]

Risques technologiques du Cloud

Les institutions financières habituées aux tests hebdomadaires de « basculement » des centres de données sur site pourraient bientôt devoir envisager de réaliser des tests de résilience similaires pour les infrastructures basées sur le Cloud. Au Royaume-Uni, par exemple, la Prudential Regulation Authority cherche comment accéder à davantage d'informations auprès des principaux fournisseurs de Cloud afin de mieux évaluer les risques de pannes techniques des services Cloud.[6]

Selon des rapports parus dans le Financial Times, un proche des régulateurs a déclaré : « Nous examinons les fournisseurs de Cloud du point de vue de la résilience opérationnelle. Avons-nous besoin d'intervenir davantage ? Comment leur faire confiance ? Nous commençons à les considérer comme des tiers critiques devant faire l'objet de plus de surveillance. »[6]

Les stratégies hybrides et multi-Cloud gagnent du terrain pour réduire le risque de points de défaillance uniques et de verrouillage des fournisseurs.

- Une étude Google Cloud souligne que 28 % des services financiers dépendent actuellement d'un fournisseur unique.
- Mais 88 % de ceux qui n'utilisent pas encore le multi-Cloud l'envisagent.[7]

Si l'on considère les obstacles techniques à la résilience opérationnelle, il convient d'évaluer les risques de verrouillage, ainsi que la facilité de répliquer des charges de travail spécifiques dans différents Clouds. La capacité de rapatriement vers une infrastructure sur site détenue doit également être prise en compte.

Risques systémiques du Cloud

Les régulateurs craignent une augmentation des risques systémiques à mesure que la proportion de services dépendant du Cloud augmente.

- Près de la moitié des charges de travail des services financiers sont désormais exécutées dans des Clouds publics.[8]
- « La dépendance croissante à l'égard d'un petit nombre de CSP et d'autres tiers critiques pourrait augmenter les risques pour la stabilité financière en l'absence d'une surveillance réglementaire directe accrue de la résilience des services fournis. »
  La Banque d'Angleterre, juillet 2021.[9]

5 https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022

6 https://www.ft.com/content/29405a47-586b-4c5a-b641-0f479b4cee1d

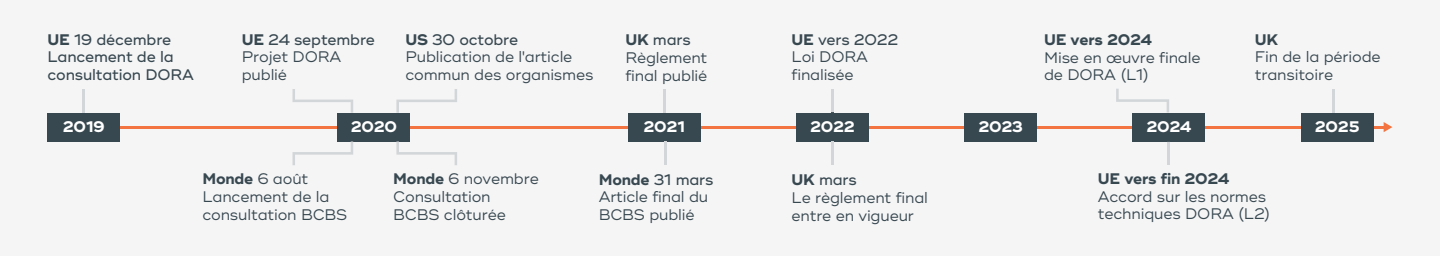
7 https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services

8 https://www.statista.com/statistics/1257930/cloud-workloads-financial-services-banking

9 https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management

teradata.

Ce que font les régulateurs



Les régulateurs du monde entier commencent déjà à agir sur ces risques.

Par exemple, au Royaume-Uni, l'une des premières juridictions à prendre des mesures, de nouvelles règles de résilience opérationnelle sont apparues en mars 2021. Elles n'ont donné aux institutions financières qu'un an pour les mettre en œuvre ; ces délais contraints obligent les entreprises à prouver leur résistance face aux impacts. La Prudential Regulatory Authority est allée jusqu'à mentionner explicitement à la fois les sous-traitants TIC et les dangers de leur concentration dans ses déclarations de politique et de surveillance (PS7/21 et SS2/21) publiées en mars 2021. L'objectif spécifique était de gérer la résilience dans un environnement axé sur le Cloud.

Ils soulignent l'importance d'éviter une dépendance excessive à l'égard d'un seul fournisseur de TIC externalisé (notamment les services Cloud) et d'éviter tout verrouillage, et d'assurer la substituabilité des services Cloud (y compris l'identification d'autres fournisseurs appropriés). Ils exigent également des preuves des mesures temporaires prévues pour poursuivre les opérations en cas de sortie urgente (« Stressed Exit ») pour quelque raison que ce soit.

D'ici la fin de la période de transition en mars 2025, les entreprises doivent être en mesure de montrer comment maintenir la résilience opérationnelle pour tout actif (notamment les données et la technologie) lié à la fourniture d'un service commercial important. La Prudential Regulatory Authority indique qu'elle ***« souhaite que les entreprises évaluent les exigences de résilience des services et des données externalisés et, en considérant les risques, qu'elles choisissent une ou plusieurs options de résilience du Cloud disponibles. »***

En Europe, où l'on a agi sans attendre, l'approche est légèrement différente. La loi sur la résilience opérationnelle numérique, connue sous le nom de DORA (Digital Operational Resilience Act), cible nombre de ces risques et c'est un pilier fondamental de la loi européenne sur la finance numérique au sens large. Elle décrit les exigences de la résilience numérique pour les entreprises, en demandant notamment des stratégies multi-fournisseurs pour les TIC et en associant les dépendances technologiques. Elle va plus loin que d'autres réglementations en étendant la surveillance aux principaux fournisseurs tiers.

Ces derniers incluent explicitement les fournisseurs de services Cloud. En fonction de l'importance et de la complexité, les entreprises devront tenir un registre de tous les arrangements contractuels fournis par les fournisseurs tiers de TIC. Les fournisseurs eux-mêmes seront soumis à une surveillance réglementaire pour garantir la mise en place des plans et des procédures visant à protéger les entreprises contre les risques technologiques.

Les délais de cette législation pourrait être allongés, mais le projet initial de DORA a été publié en septembre 2020 et le projet final est attendu en 2022 à l'issue d'un débat entre le Parlement européen, le Conseil et la Commission. L'application est prévue un an après l'adoption de la loi. En parallèle, d'autres améliorations et extensions (de niveau 2) devraient être publiées prochainement en vue d'une discussion et d'un accord dans les 2 ou 3 ans. Cela aura des impacts significatifs sur la manière dont les institutions financières européennes contractent et gèrent leurs fournisseurs de services Cloud. Il leur est donc conseillé de commencer à se préparer dès maintenant.

Les régulateurs britanniques et européens ont jusqu'à présent mis en place les mesures les plus avancées en matière de résilience opérationnelle. Cependant, d'autres juridictions dans le monde, y compris les États-Unis, commencent à mettre en œuvre des mesures similaires. Les organisations doivent suivre les réglementations locales sur la résilience opérationnelle sur les marchés où elles opèrent, mais il semble que la réglementation se renforcera dans ce domaine.

teradata.

Il est judicieux de répondre à présent aux questions difficiles

Quelles que soient les évolutions réglementaires, les entreprises doivent afficher leur résilience opérationnelle en cas de sortie urgente et imprévue d'un service Cloud. Les régulateurs exigeront de voir des plans détaillés et leur efficacité prouvée par des tests rigoureux. Les règles publiées et le règlement proposé par la Prudential Regulatory Authority[10], la BCE[11] et la Réserve fédérale[12] pointent vers plus de tests dans ce domaine. Mais les institutions financières peuvent se préparer à ces exigences tout en développant les plateformes de données évolutives, rapides et flexibles dont elles ont besoin pour être compétitives dans le monde numérique.

L'interrogatoire serré des régulateurs portera sur le cœur des stratégies Cloud des entreprises et leur capacité à faire face à des chocs soudains allant des « pannes » du Cloud aux désaccords contractuels et à la faillite des fournisseurs. Du point de vue des données, ils voudront tester les plans d'accès et d'utilisation des données de l'ensemble de l'organisation pour soutenir l'analyse et la prise de décision automatisée, même en cas de panne prolongée d'un fournisseur de services Cloud.

Savoir où se trouvent les données, quels services commerciaux importants dépendent de quels ensembles de données et où s'exécutent les modèles d'analyse cruciaux est la première étape fondamentale pour renforcer cette résilience. Les principales organisations ont déjà pris de l'avance pour répondre à ces questions. Permettre la libre circulation des données dans l'entreprise pour les utiliser de manière innovante afin de créer de nouveaux services et améliorer l'expérience client est au cœur de la transformation numérique sectorielle. De ce point de vue, les exigences du régulateur de démontrer la résilience opérationnelle sont des avantages supplémentaires de ces projets en cours.

Au lieu de considérer la surveillance accrue des régulateurs et la nécessité de développer une résilience opérationnelle pour gérer la perte de fournisseurs de services Cloud « trop gros pour faire faillite » comme une tâche onéreuse, les entreprises peuvent voir ces demandes comme un signal supplémentaire pour accéder à une infrastructure de données efficace.

Liste de contrôle de la résilience opérationnelle

Les données et l'analyse des données doivent être totalement prises en compte dans vos plans de résilience opérationnelle. Avez-vous posé les bonnes questions et êtes-vous satisfait des réponses reçues ?

- Avez-vous discuté des plans de sortie avec vos fournisseurs de services Cloud ?
- Proposent-ils des clauses contractuelles conformes qui facilitent les dispositions d'une sortie urgente ?
- Avez-vous examiné les engagements de sécurité, de récupération et de restauration des CSP ?
- Savez-vous où se trouvent toutes vos données ?
- Avez-vous analysé le positionnement de la charge de travail ?
- Pouvez-vous associer les dépendances des données des services commerciaux importants ?
- Pouvez-vous identifier toutes les charges de travail d'analyse de données essentielles pour les services commerciaux importants et savez-vous où elles s'exécutent ?
- À quelle vitesse pouvez-vous répliquer des modèles d'analyse sur d'autres plateformes ?

10 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B414730C697DC8BEB353F3EE5A628

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-_en

12 https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

teradata.

Ce que vous devez faire maintenant

De nombreuses institutions financières ont déjà opté pour des approches multi-Cloud. Que ce soit pour des raisons financières ou opérationnelles, ou pour répondre à des charges de travail et des technologies spécifiques, une approche multi-Cloud constitue la base de la résilience opérationnelle. Cependant, à elles seules, les architectures multi-Cloud peuvent être insuffisantes. Des obstacles techniques, financiers et contractuels peuvent entraver le déplacement des charges de travail d'un Cloud vers un autre.

L'ajout (ou le maintien) d'une infrastructure sur site peut renforcer la résilience. Conserver la capacité de fournir des services critiques à partir d'une infrastructure propre sous le contrôle direct de la banque peut servir de tampon si les ressources Cloud deviennent inaccessibles pour une raison quelconque.

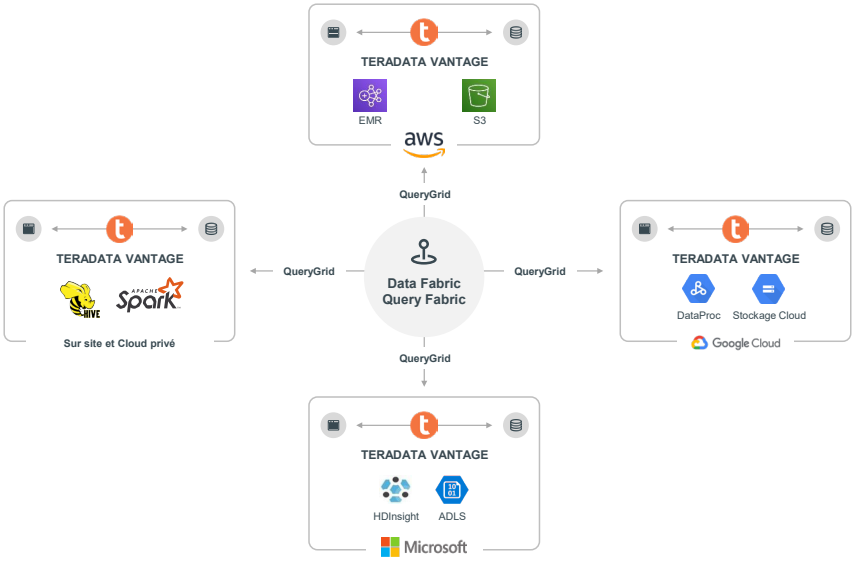
Combiner les deux approches avec un environnement de données Cloud connecté offre une solution. La création d'une plateforme de données fonctionnant de manière transparente avec les Clouds de n'importe quel fournisseur et avec des solutions sur site offre une résilience opérationnelle et la flexibilité nécessaire pour poursuivre de manière rentable sa transformation numérique. Une telle solution peut connecter et synchroniser les données de n'importe quelle application et prendre en charge les besoins en données de l'entreprise, de l'entreposage de données de base aux analyses avancées.

À quoi cela pourrait ressembler

Des organisations du monde entier exploitent les performances et l'évolutivité multidimensionnelle de Teradata pour créer des plateformes de données Cloud à l'échelle de l'entreprise qui répondent à leurs besoins analytiques en constante évolution. Tel un référentiel central unique intégrant les données de n'importe quelle source, Teradata garantit la circulation adéquate des données. Comme l'illustre le schéma ci-dessous, elles peuvent également se connecter à n'importe quel fournisseur de services Cloud tout en conservant des capacités sur site. La flexibilité nécessaire pour maintenir des options de transformation numérique est là et les exigences en matière de résilience opérationnelle sont respectées.

Résilience opérationnelle

Schéma architectural expliquant comment alterner facilement entre plusieurs fournisseurs de Cloud et revenir sur site pour assurer la continuité des activités. La plateforme de données multi-Cloud hybride de Teradata augmente votre flexibilité et vous évite tout blocage auprès d'un seul fournisseur de Cloud public.



Révision de l'exactitude technique Février 2022

Un data fabric à haut débit connecte les charges de travail dans un environnement hautement distribué.

Le choix du point d'entrée permet de générer des requêtes à grande échelle sur n'importe quel système de la structure, sur site et dans plusieurs environnements de Cloud public.

Le traitement Pushdown permet de minimiser les coûts de transfert et de sortie des données en déplaçant les requêtes pour qu'elles s'exécutent au plus près des données.

teradata.

Un monde hybride et multi-Cloud

Les organismes financiers adoptent rapidement le Cloud comme base de modèles commerciaux agiles centrés sur le client. Ils réduisent ainsi leurs coûts et bénéficient de la flexibilité nécessaire pour répondre aux environnements client et économiques instables, et peuvent prévoir et planifier les prochaines vagues de changement. Mais les Clouds eux-mêmes ne sont pas statiques. Dans le cadre de leurs stratégies, les institutions financières doivent évaluer attentivement et surveiller en permanence les risques concernant la résilience opérationnelle implicite dans les infrastructures Cloud.

Il existe des risques commerciaux, technologiques et systémiques et les régulateurs sont déjà inquiets. L'Europe et le Royaume-Uni ont commencé et d'autres pays vont suivre. Les grandes organisations anticipent et se préparent déjà à une réglementation inévitable. Il est temps d'agir.

Il est possible de limiter les risques opérationnels associés au Cloud par une approche hybride multi-Cloud conservant flexibilité et résilience.

Aujourd'hui, Teradata travaille avec des institutions financières du monde entier pour intégrer la résilience opérationnelle dans leurs stratégies Cloud.

L'approche multi-Cloud hybride de Teradata renforce la résilience opérationnelle en offrant la flexibilité nécessaire pour déplacer les données et les charges de travail de manière transparente entre les Clouds, et de n'importe quel Cloud vers une infrastructure sur site, selon les besoins. Elle peut prendre en charge les sorties planifiées ou les sorties urgentes d'un Cloud et, en cas de panne, les données peuvent être rapidement restaurées sur n'importe quel système sur site ou Cloud, pour une reprise quasi immédiate des opérations.

L'approche hybride et multi-Cloud de Teradata est intéressante pour tout organisme financier cherchant à prospérer dans un monde numérique en évolution. Avec tous ces avantages et des capacités de résilience opérationnelle améliorées, de nombreux organismes financiers se tournent vers Teradata pour planifier et exécuter leurs stratégies d'atténuation des risques.

À propos de Teradata

Teradata exploite toutes les données, tout le temps, pour que vous puissiez tout analyser, déployer des solutions n'importe où et fournir les analyses qui comptent le plus pour votre entreprise. En répondant à la complexité, au coût et à l'inadéquation des analyses d'aujourd'hui, Teradata transforme l'activité des entreprises et la vie des personnes. Trouvez les réponses que vous cherchez sur Teradata.com

Auteur

Graham Corr consultant principal du secteur, pratique des services financiers, zone EMEA

17095 Via Del Campo, San Diego, CA 92127 Teradata.com